

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR SEARCH AND SEIZURE WARRANT**

I, Lane Thorum being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property— a digital device—which is currently in law enforcement possession (the “Device”), as described in Attachment A, and the extraction from that property of electronically stored information as described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”), and I have been in this position since April of 2022. I am currently assigned to the Cleveland Division of the Federal Bureau of Investigation, specifically the Joint Terrorism Task Force. Based on my training and experience, I know that it is common for individuals to use their cell phones to browse the web, make internet purchases, and communicate with others. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

4. This affidavit is submitted in support of an application for a search warrant for evidence, fruits, and instrumentalities regarding violations of 18 U.S.C. § 922(g)(1) (felon in

possession of a firearm) via forensic examination of the Device and 18 U.S.C. § 875 (interstate communications) via forensic examination of the Device.

5. As discussed herein, there is probable cause to search the Device, further described below and in Attachment A, for the things described in Attachment B.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

6. The property to be searched is a black in color Samsung S23 cellular phone, IMEI: 351059812460609, that is, the “Device.” The Device is currently located at 1501 Lakeside Ave, Cleveland, Ohio 44114.

PROBABLE CAUSE

7. On August 17, 2023, the Wickliffe Police Department began receiving a number of 911 calls reporting gunshots in the area of Ridgewick Drive, Wickliffe, Ohio. Officers arrived on scene, interviewed neighbors, and determined that a man exited 1548 Ridgewick Drive, fired multiple rounds into the air, and then returned inside. Neighbors also reported that the resident’s girlfriend was inside. Officers were able to determine that the resident was DANIEL KOVACIC. KOVACIC’s next door neighbor told officers that two weeks prior, he and KOVACIC got into a verbal argument about KOVACIC’s music being too loud. KOVACIC pulled out a pistol, “racked the slide,” and pointed it at the neighbor’s chest.

8. Shortly after officers arrived on scene, a female, KELLY SIEBERT, exited the residence and spoke with officers. SIEBERT explained that while she did not hear any gunshots, she has seen a gun in KOVACIC’s home before, located in the couch. She explained that it was not her gun and that no one else had been in the home during that time.

9. While police were speaking to SIEBERT, KOVACIC's mother called her phone. The police spoke to KOVACIC's mother who stated that KOVACIC was undergoing some sort of mental crisis and abusing narcotics. KOVACIC's mother stated that on this date KOVACIC had sent her several disturbing text messages in which he threatened to kill "the enemies of the white race."¹ (*Figure 9, 10, 11*). The time stamp on the messages indicate that they were sent at approximately 5:30 pm while police were on the property surrounding the residence. KOVACIC's father called Wickliffe police and stated that approximately 1 week earlier, he requested KOVACIC take a drug test, which came back positive for cocaine. Police also made contact with KOVACIC's boss, who stated that he had terminated KOVACIC on this date after a client reported that the defendant had been intoxicated and unprofessional. KOVACIC's boss provided the text communications with KOVACIC to the police.

10. The Emergency Response Team responded on scene and attempted to make contact with KOVACIC for multiple hours by calling his cell phone and using a PA system unsuccessfully. Several hours after the standoff began, officers observed KOVACIC in the upstairs window and ordered him to come to the front door, which he complied and was taken into custody without incident.

11. Wickliffe Police Department executed a search warrant on KOVACIC's residence at 1548 Ridgewick Drive. Inside, officers found a fully loaded Sig Sauer, Model P238, .380 caliber pistol bearing serial number 27B206165 (*Figure 1*) located between the back of the couch

¹ While police were executing a search warrant at Kovacic's residence, they observed Nazi memorabilia inside and the FBI has identified Kovacic as being connected to at least two white supremacist groups.

and a couch cushion in the living room (*Figure 2*). An Uncle Mikes firearm holster for the Sig Sauer was found on the armrest of the couch (*Figure 3*). Furthermore, inside a pair of shorts located on the floor of the living room was a 9mm magazine loaded with seven rounds of 9mm ammunition (*Figure 4*). In KOVACIC's bedroom, officers found a black plastic Sig Sauer gun case bearing the serial number 27B206165, with 1 round of .380 ammunition, and 32 rounds of 9mm ammunition (*Figure 5*). They also found a plastic gun holster that appeared fit the Sig Sauer (*Figure 6*). Outside of the residence, officers found two spent .380 caliber shell casings (*Figures 7 and 8*).



Figure 1

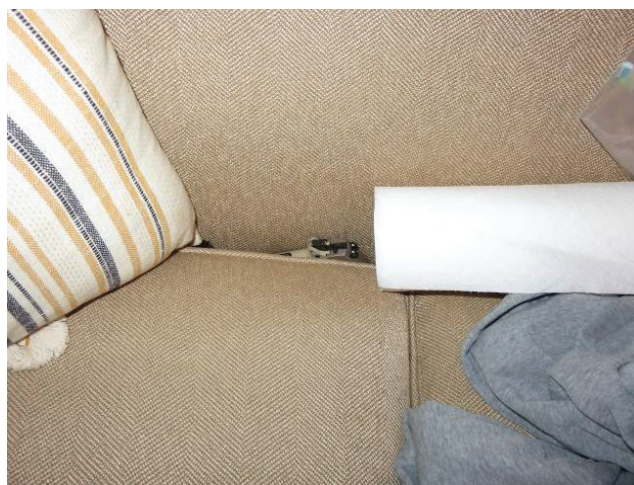


Figure 2



Figure 3

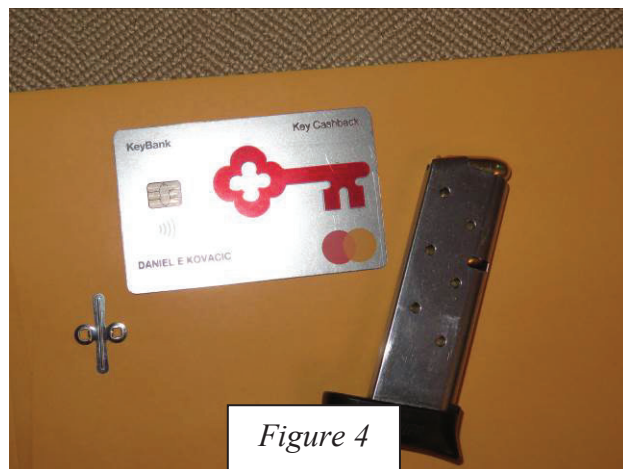


Figure 4



Figure 5



Figure 6

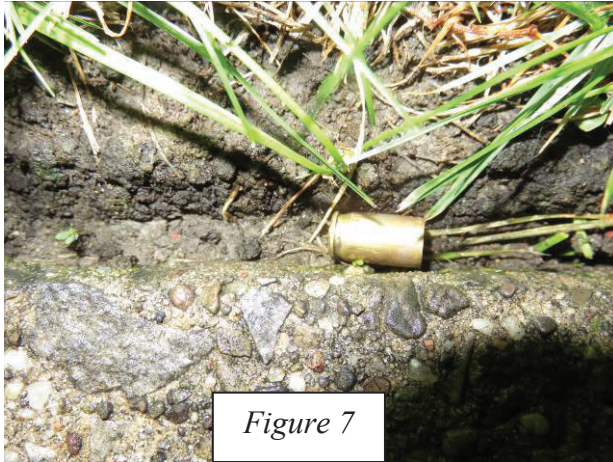


Figure 7



Figure 8

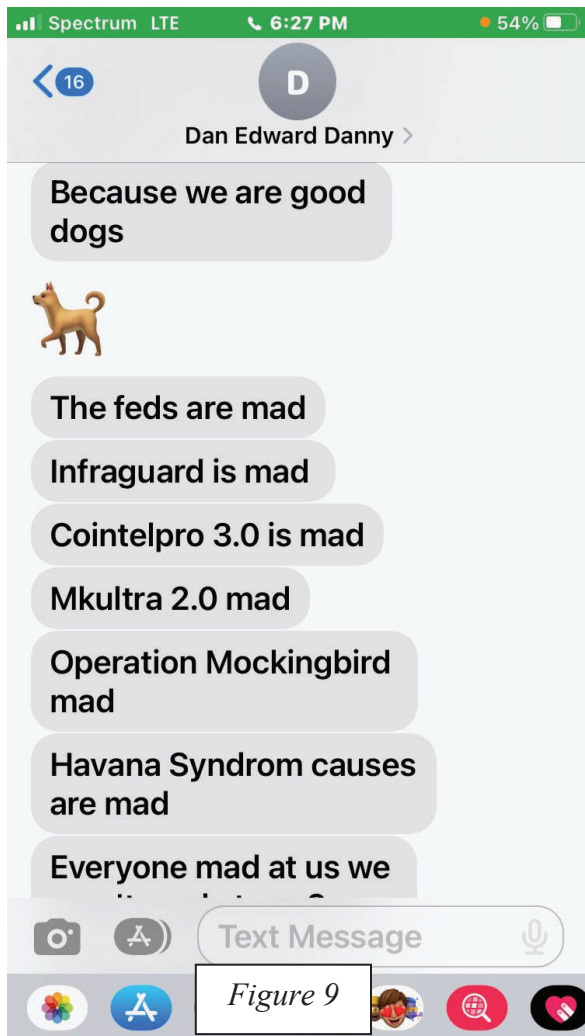


Figure 9

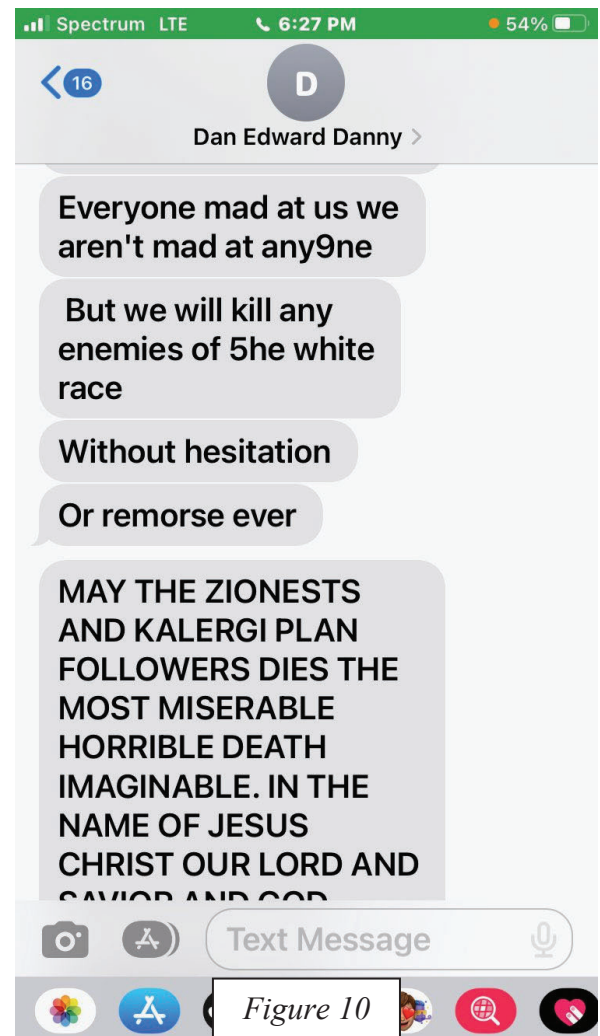
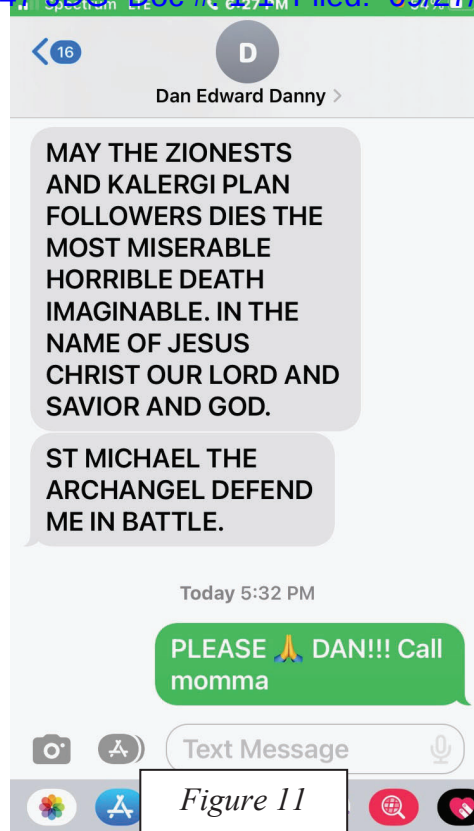


Figure 10



12. KOVACIC has knowingly been convicted of two crimes that are punishable by imprisonment for a term exceeding one year: felonious assault, a felony of the second degree, on or about May 24, 2010, in Case Number 09-CR819, in the Lake County Court of Common Pleas; and Assault on a Peace Officer, a felony in the fourth degree, on or about February 4, 2010, in Case Number 09-CR-546, in the Lake County Court of Common Pleas. KOVACIC is therefore prohibited from possessing a firearm.

13. On September 19, 2023, Bureau of Alcohol, Tobacco, Firearms and Explosives (“ATF”) Special Agent John M. Laurito examined the items seized from KOVACIC’s residence. Special Agent Laurito has been employed with the ATF since 2000. He renders advice and assistance to law enforcement officers and other federal agents concerning the identification, origin, markings, function, and history of firearms. Special Agent Laurito has completed the ATF’s Firearms Interstate Nexus Training Course in Martinsburg, West Virginia, as well as the ATF Advanced Firearms Interstate Nexus Course and ATF Advanced Ammunition Interstate

Nexus Courses. Special Agent Laurito also performs firearm traces through the ATF National Tracing Center concerning the manufacture and interstate shipment of firearms. Special Agent Laurito prepares reports relating to the identification, origin, and classification of firearms and ammunition under the provisions of federal law. Special Agent Laurito examined the firearm and ammunition seized by Wickliffe Police on August 17, 2023. Special Agent Laurito confirmed that the Sig Sauer pistol, model P238, .380 caliber, serial number 27B206165 is a firearm under federal law and was not manufactured in the State of Ohio, and that the ammunition was also not manufactured in the State of Ohio. Therefore, based upon my training and experience and Special Agent Laurito's training and experience, there is probable cause to believe that the pistol and ammunition seized from KOVACIC's home crossed a state line prior to KOVACIC's possession of them.

14. ATF provided records regarding the purchase history of the firearm, which revealed that it was purchased by a ANDREW JOHN REID on March 3, 2021 who identified his address in Mentor, Ohio.

15. On September 20, 2023, a Federal Grand Jury returned a true bill indictment for one count of 18 U.S.C. § 922(g)(1) for KOVACIC.

16. On September 27, 2023, FBI special agents arrested KOVACIC at the Willoughby Municipal Courts located at 4000 Erie Street, Willoughby, OH 44094. KOVACIC was searched incident to arrest, which revealed the Device on his person. The Device was seized and entered into evidence according to FBI policy at 1501 Lakeside Ave, Cleveland, OH 44114.

TECHNICAL TERMS

17. “Wireless telephone” (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through “wi-fi” networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional “land line” telephones, computers, and other digital devices. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system (“GPS”) locating and tracking technology, and accessing and downloading information from the Internet.

18. The “Internet” is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

19. Based on my training, experience, and research, the Device has capabilities that allow it to serve as a wireless telephone, digital camera, and internet browser. In my training and experience, examining data stored on devices of this type can uncover, among other things,

evidence that reveals or suggests who possessed or used the device, and sometimes by implication who did not, as well as evidence relating to the commission of the offense(s) under investigation.

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

20. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found within the Device, in whatever form they are found. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that there is probable cause to believe that the records and information described in Attachment B will be stored in the Device for at least the following reasons:

a. Individuals who engage in criminal activity, including 18 U.S.C. § 922(g)(1), use digital devices, like the Device, to access websites to facilitate illegal activity and to communicate with co-conspirators online; to store on digital devices, like the Device, documents and records relating to their illegal activity which can include logs of online chats with co-conspirators; email correspondence; text or other “Short Message Service” (“SMS”) messages; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social medial accounts. Further, I know in my training, knowledge, and experience that those engaged in the sales and/or exchange of firearms use cellular phones as a necessary tool of exchange to arrange meet locations, negotiate prices with seller and purchaser. This can include but is not limited to receipts of purchases/exchanges, websites for research/reference, and communications.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often “back up” or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person “deletes” a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from a digital device depends less on when the file was downloaded or viewed

than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

21. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard

drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate

conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

22. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have

specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Recovery of “residue” of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and

extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting “keyword” search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format (“PDF”), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large,

and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as “AES-256 encryption” to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, “Hide It Pro,” disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests

permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

23. In searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

a. The digital device, and/or any digital images thereof created by law enforcement, sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

b. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by “opening,” reviewing, or reading the images or first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic “keyword” searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

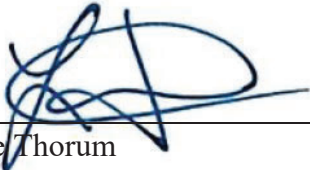
c. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition,

the forensic examiners may search for and attempt to recover “deleted,” “hidden,” or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the Device(s) will be specifically chosen to identify the specific items to be seized under this warrant.

CONCLUSION

14. I submit that this affidavit supports probable cause for a warrant to search the Device described in Attachment A and to seize the items described in Attachment B.

Respectfully submitted,



Lane Thorum
Special Agent
Federal Bureau of Investigation

This affidavit was sworn to by the affiant by telephone after a PDF was transmitted by email, per Crim. R. 41(d)(3), on this 27th day of September 2023.



JONATHAN D. GREENBERG
UNITED STATES MAGISTRATE JUDGE

